**Converged Networking and Fiber Channel over Ethernet: A Primer for the SAN/Storage Engineer**

**Intended Audience**

This document is intended for a SAN Engineer who design for or deploys Storage, Networking, and Virtualization technologies. It provides a sound understanding of what Converged Networking and FCoE are, and how they work. The aim of this technical document is to help alleviate any doubt of FCoE, provide a great high-level understanding of how FCoE works, and prepare the reader for any upcoming training pertinent to Converged Networking. This technical document assumes that the reader has a good understanding of Storage Technologies, experience deploying iSCSI and Fiber Channel SANs, knowledge of Virtualization, and good knowledge in Networking (enough to be able to deploy an iSCSI SAN with Ethernet Switches). If the reader is unfamiliar with most technical terms, there is a glossary they may review prior to fully reading this document.

**Introduction to Converged Networking**

Converged Networking is the unification of LAN and SAN over a dual, highly-available, redundant fabric. When the word “Fabric” is used, it refers to a Switch capable of forwarding Ethernet and Fiber Channel Frames.

Data Centers are evolving to implement Converged Networking in order to reduce:

* PCIe Adapters on a Host - Instead of having a minimum of two NICs, and two Fiber-Channel Host-Bus Adapters, consolidation allows the use of a singular Converged Network Adapter (CNA) with two 10 Gigabit per second ports. The CNA will be discussed further on.
* Cabling - Instead of two Ethernet cables, and two FC Fiber-Optical cables, these can be replaced with two 10Gb CAT6A, or 2 TwinAx 10Gb. (CAT6A Cabling may be subject to errors).
* Cooling Costs and Requirements – Potentially, half of network devices are removed, means less heat generation, therefore less cooling requirements.
* Reduction in Power Requirements – Less power required since less ToR Switches (cut them in half)
* Management Overhead and Complexity – Focus on managing less switches, and HBAs. Less complexity in topological map of network

The use of Converged Networking implies that a single cable connecting from a Server to a fabric will carry both Storage and LAN traffic. Of course, in a typical data center, high-availability is crucial and key.

The traditional LAN and SAN infrastructure consists of multiple switches, storage targets, and end hosts with both Ethernet NICs and iSCSI or Fiber Channel HBAs. On Field Deployments, it’s quite common to walk into environments where a customer has all of their servers attached to the rest of the network using standard Cat5e/Cat6 cabling. The hosts are then connected to a Storage Area Network, which only carries storage-related traffic (commands and data). Although the traditional LAN and SAN environment may appear to be the safer choice, this impedes taking advantage of the benefits mentioned earlier.

Converged Networking isn’t limited to unifying Fiber Channel and LAN traffic across the same fabrics, it also applies to the use of iSCSI and LAN traffic over the same set of Ethernet Switches. iSCSI is easier to integrate into an environment since it relies on the OSI Model, and uses TCP (port 3260) over IP over Ethernet. Because iSCSI is TCP/IP based, TCP has a mechanism for for retransmission of packets when they do not arrive at the destination. The TCP retransmission may be suitable for regular LAN traffic however, with a high percentage of retransmission, higher latency is experienced, which is unacceptable for storage traffic.

Throughout this document, FCoE, DCB and Converged networking will be explored in much more detail.

**High Availability**

When High Availability is discussed, it simply means that a service should be running all the time. When a Data Center is designed as per best practices, no single point of failure should exist, and with that, High Availability is present. A Data Center would not house 1 ESXi host for many multiple machines; at least two would be present. The same principle would apply to a converged network: no single points of failure. The aim is for redundancy right throughout a network, converged or not.   
  
Specifically for Converged Networking, the ideal setup would entail having hosts connect redundantly to Top of Rack (ToR) switches. This principle of redundancy originates with having multiple paths to storage, with redudant fabrics.

**Before we get to FCoE: Fiber Channel**

Fiber Channel originates from the idea where a channel is used to create a point-to-point connection between an Initiator and a Target. The Initiator would typically be a computer or server, which directly connects via a SCSI cable out to a Target, which would an array of some sort. Some of the limitations of this topology are that it’s not scalable, it’s a single point of failure, and it’s distance limited. In addition to this, SCSI was very sensitive to latency and dropped frames. Fiber Channel over came these limitations by allowing for various topologies (Ring, Star, Point-to-Point).

Fiber Channel enabled the scalable use of SCSI as a Storage Block-based Protocol. FC is able to go the distance SCSI could not; it could be built with varying topologies, which is tied with eliminating the single point of failure. FC was created built in mechanisms to ensure lossless connectivity and endure latency issues through a method called Buffer-to-Buffer (B2B) credits. B2B Credits allow a sender to send as many Fiber Channel frames as the receiver will allow. For example, if the receiver allows a sender to send 4 FC frames, then the sender will transmit 4 FC Frames. The Sender will not send more frames because a Pause is in place to prevent more transfers. If the Pause did not exist, and the sender kept transmitting frames, too many for the receiver to handle, frames will be dropped. This does harm the flow of traffic, and essentially destroys the Point-to-Point SCSI connections and commands.   
  
Similarly, Flow Control is used in Ethernet networks and, Priority Flow Control is used in FCoE or iSCSI networks; more on this later.

FC is a very large topic to discuss, however some of the facts below are pertinent to understanding FcoE:

* **Fiber Channel frames** typically have a MTU size of 2148 bytes, with a maximum payload size of 2112 Bytes.
* The processes for establishing a virtual point-to-point connection between initiator and target:
  + **First - FLOGI** (Fabric Login): The Host or Array logs into the Fabric; it simply tells the FC Switch that it has joined in part of the fabric services
  + **Second - PLOGI** (Port Login): The host and array establish a virtual or logical, point-to-point connection
  + **Third - PRLI** (Process Login Process): This is where the communication of SCSI commands, carrying of SCSI frames, and data transfers has occurred.
* **RSCN** (Registered State Change Notification): Anything that occurs in the fabric such as a port connect/disconnect, a FLOGI, a PLOGI, is communicated out to every other device on the fabric.
* **Domain IDs and FCIDs**: These two components are very important for several functions of the fabric
  + **Domain IDs** are used to identify each FC-Switch in the total fabric
  + **FCIDs** (Fiber Channel IDs) are created and assigned to every single device in the fabric, whether it be a host, a switch, or a storage device. FCIDs. One can almost equate a FCID to an IP address. FCIDs are typically used to route Fiber-Channel frames throughout the Fabric. The FCIDs help dictate the best path from Point A to Point B in a given fabric.
  + **FSPF** (Fabric Shortest Path First): Is the protocol by which FC frames are routed using the FCID and Domain ID addressing.
* **Common Fiber Channel Port Types**: A number of these varying ports exist however, some are more common in the Data Center
  + N\_Port – Node Port. This type of port is typically found on an HBA port of a server system. It can connect either to an F\_Port or an N\_Port.
  + F\_Port – Fabric Port.This type of port is typically found on a Fiber Channel Fabric Switch.
  + E\_Port – Expansion Port. Commonly used for ISLs between switches.U\_port (Brocade only)
  + TE\_Port (Cisco, and Brocade) – Trunking Expasion port. This is commonly used when multiple VSANs or vFabrics are present in a switch. They pass through the TE\_Port over to another Fabric.
  + U\_Port – Universal Port – A port that can become any other port type depending on the other end of the link. Typically a port sits in a U\_Port state until something is plugged in.
  + G\_Port – General Port. A port type which, similar to a U\_Port, can become any other port type (N\_Port, F\_Port). This port type is common after an optical cable is plugged into that port on the switch.
  + NP\_Port – Node Proxy Port. This port type often pairs up with a F\_Port. The NP\_Port typically originates from an Fiber Channel switch operating in Access Gateway Mode (Brocade), NPV Mode (Cisco), or NPG Mode (NPIV Proxy Gateway, Dell). The NP\_Port typically enables the switch to act like a “Host” and conducts FLOGIs on behalf of downstream devices. This way, the switch itself does not consume a domain ID.
* **FC Port Types (Uncommon)**
  + FL\_Port – Fabric Loop Port. This is less common in a Data Center strictly because the toplogy it follows is a Ring topology. It does not quite scale very well and, lacks redundancy. Commonly found on a Fabric Switch port.
  + NL\_Port – Node Loop Port. Similar to above except, it is found on a Host/Server HBA, or FC-capable JBOD.
* **Zoning and Access Control**
  + Port Zoning – As zoning is quite a familiar topic, the idea is simple: Control which initiators can talk to which targets at a port level. Zoning can be done to allow devices connected to certain ports to talk to each other. If a device is moved to another port on the FC Switch, zoning parameters need to be modified.
  + WWN Zoning – Another form of zoning by which a device can be moved along any switchport such that it maintains it’s pWWN (port World Wide Name). It is a control mechanism to ensure devices are only allowed to talk to whomever else is contained within that same zone
  + Hard vs. Soft Zoning – Although some vendors may make Hard and Soft Zoning synonymous to Port and WWN zoning, respectively, this is not the case. Hard zoning is typically done in hardware, and at the switch level. Soft zoning is typically done at an array level. Although it may seem confusing, most of the time, the concept of Hard vs. Soft zoning can be disregarded.
  + Aliases – A human readable name that is created and mapped to a WWN
  + Zoneconfig, Zoneset – A list of zones which are contained in a set, ready for activation and use for Fabric Services.
* **Fiber Channel Link Speeds**
  + FIber Channel Link speeds can vary; they start from 1Gbps, and work its way up to 32Gbps
  + 1, 2, 4, 8, 10, 16, and 32Gbps are available, with 8Gbps and 16Gbps being quite common in the Data Center.

**And then there was Ethernet**

Everyone who works in the Technology Industry is likely to be very familiar with Ethernetlo, has heard the term, or is actively working with it. Ethernet is an IEEE 802.3 standard which falls under Layer 2 of the OSI model. Where Layer 1 is medium, and bits trasmission, Layer 2 is the level above which takes Layer 1 information and encapsulates it for transmission. The transmission typically occurs across a local segments. When a CAT5E or CAT6 cable is plugged from a computer and to a switch, Layer 2 communication occurs where the switch discovers the computers globally significant MAC address. Ethernet traffic, or Frames, are transported from device to device. The way frames are transported are based on a switch’s forwarding table. Each switch has something called a Content Addressable Memory Table (CAM Table), or a MAC Address Table. The table is simplististic in the sense that it contains a few pieces of information on a MAC address: the MAC address itself, which port it was learned from, and which VLAN the MAC address resides in. To understand the forwarding decision, here is an example:

|  |  |  |  |
| --- | --- | --- | --- |
| **Host** | **MAC Address** | **Port Origination** | **VLAN** |
| Windows01 | 00:00:00:00:00:01 | TenGigabit 0/1 | 1 |
| ESXi02 | 00:00:00:00:00:02 | TenGigabit 0/5 | 3 |
| Linux03 | 00:00:00:00:00:0A | TenGigabit 0/20 | 1 |
| Xen04 | 00:00:00:10:00:C0 | TenGigabit 0/36 | 3 |

Because the table displays what MAC Address came from which port, and which VLAN it is a member of, the switch can determine which to port it should forward the frame. For Example, Xen04 and Windows01 cannot communicate because they aren’t on the same VLAN. Windows01 and Linux03 can communicate so, if Windows1 were to ping Linux03, Linux03 would reply back to the ping (a successfully communication). The switch would forward these frames based on the table. In order for devices to communicate between VLANs, a router would be required. Routing and routers are a separate discussion altogether. For FCoE, IP routing is not supported strictly because routing adds latency, which is bad for FCoE.

As Ethernet is a Layer 2 transport technology, it is able to carry FC-frames within it and thus, forward frames as normal. In addition to this understanding of Ethernet, each Ethernet Frame has the ability to say what kind of frame it is. There is an “EtherType” header in each frame, which is a 2-Byte value, in hexadecimal. The common types are:

* 0x0800 – IPv4
* 0x0806 – ARP
* 0x8870 – Jumbo Frames
* 0x8906 – FCoE (for the Data Plane)
* 0x8914 – FIP, FCoE Initialization Protocol (for the Control Plane)

To simply put this, the EtherType header will suggest if the traffic is LAN, Control Plane, or FCoE.

**Fiber Channel over Ethernet**

Although there are many definitions to Converged Netowrking, the context of this technical paper is limited to converging or unifying SAN and LAN traffic across the same network, and wire.

The concept is very simple: take Fiber Channel Frames and encapsulate them into an Ethernet frame. If designed and implemented carefully, a Field Engineer will only see two TwinAx, Cat6A, or Fiber Patch cables going from a server to a pair of switches. Additionally they may either see Fiber Patch cables (if only an FC-SAN), going from the SAN to switches. In some cases, the SAN Controllers may even have Cat6A or TwinAx going to switches.

Visually, the phyically infrastructure may look very similar to a setup of an iSCSI SAN, and cabling to hosts. The difference is that FCoE the transport protocol. IT enables Fiber Channel traffic to traverse Ethernet switches capable of forwarding Fiber Channel Frames.

**FCoE Components**

FCoE, as a protocol and technology, is comprised of multiple components in order to function and present storage. It is also broken down into two sub-protcols:

* FCoE – Fiber Channel over Ethernet. The actual protocol which contains a data payload encapsulated in an FC frame, further encapsulated in an Ethernet Frame
  + An FCoE Host is given a Fabric Provided MAC Address, which is assigned by the FCF. This FMPA is used for FCoE Communication between nodes and targets
* FIP – FCoE Initialization Protcol. The protocol which ensures an establishment of communication between an initiator and target by use of “virtual links”. It is also used to discover the FCoE VLANs, and Fabric IDs. Further more, it ensures maintenance of the FCoE toplogy and checks frequently for availbility of ENodes and FCFs.
  + An ENode simply is a host with both a pWWN and nWWN

**CNA – Converged Network Adapter**. A CNA is commonly used in FCoE topologies, and can be installed in either a Server, or a Storage Array Controller (if supported). The CNA is capable of up to 10Gbps per port. The CNA looks very similar to a regular 10Gbps NIC card however its functionality is slightly different, and has characteristics of a Host Bus Adapter (HBA). On a CNA, there are two protocol stacks: one for Ethernet, and one for Fiber Channel. Depending on the manufacturer, some CNAs function differently on whichever Operating System is employed. On a VMware ESXi 5.5 host with a two-port CNA from Broadcom, one would find two 10Gbps adapters in the Network Adapters section, and two Fiber Channel ports with WWNs under the Storage Adapters Section. Of course, without a server platform, the CNA has no use.   
  
So, from two physical CNA ports, an ESXi host would see two NICs and two FC-HBAs. How is bandwidth allocated? Bandwidth is addressed in multiple way by use of DCB, NPAR, Network IO Control. There are various options to control bandwidth however, the option chosen is dependant on which CNA vendor is used.

**Fiber Channel Forwarders (FCF) –** FCFs are commonly known as Converged Switches. They function as both an Ethernet Layer-2 switch, and Fiber Channel Switch. Remember that FCoE is simply Ethernet frames that contain FC frames. When a FCF receives an Ethernet frame, it looks inside to see the contents; more specifically it looks for an EtherType. The EtherType field will dictate whether the frame is for the LAN/Network or if the frame is FCoE or FIP. If destined for LAN, the switch will forward appropriately, however if the frame indicates that it’s FCoE-related, Fabric Services or further forwarding may take place.

Because an FCF has characteristics of a Fiber Channel Switch, it has the capabilities to perform Fabric Services such as FLOGI/PLOGI or zoning. When a FCoE frame arrives at the FCF, if it is FCoE and not FIP, the frame is decapsulated to reveal the FC Frame. The FC frame is then processed as if it were on a FC switch, and forwarded to its destination: an FC SAN connected to the switch, or upstream to another FC switch.

**Fiber Channel SAN** – What good is an FCoE network without a Fiber Channel SAN? This is Storage Array capable of communicating to multiple hosts and providing them storage through the Fiber Channel Protocol. Although the array isn’t required to actually have CNAs, the FC ports of the array can either be connected to the FC-Ports of a FCF or ports on a FC Switch. An example of a FC-SAN is the Dell Storage SC8000 with Fiber Channel HBAs.

**FCoE Transit Switch –** FCoE Transit switches are typically standard ethernet switches which run FIP and DCB. They serve the purpose of only forwarding regular Ethernet LAN traffic and FCoE frames. These transit switches are also commonly called **FIP-Snooping Bridges (FSB)**. Breaking down FSB, FIP is the FCoE protocol which controls the establishment of virtual links between intiators and targets. The Snooping portion simply implies that the switch is “snooping” or looking for FIP and FCoE frames. The “Bridge” of FSB is simply another term for switch. Before switches, there were bridges, and before bridges there were hubs. It’s very common for Network Administrators to use the term Bridge in place of Switch. Examples of a FCoE transit switch (or FSB) are Dell Networking MXLs, and Dell Networking S4810/S4820 switches. If the reader was paying attention earlier, they would remember that an FC frame would typically be the size of 2148 Bytes. An FCoE frame size range anywhere from 2180 to 2500 Bytes in MTU size. Although the use of Jumbo frames (9000-12000 bytes) can be enabled on the switches, there is no added benefit as compared to using 2500 Byte “baby-Jumbo” frame.

**Data Center Bridging (DCB)** – Data Center Bridging is a technology which intends to provide lossless communication of LAN and/or SAN traffic from Node to Node. DCB Has many applications however, for the purposes of this Primer, DCB is used for lossless iSCSI and FCoE Traffic. DCB originated from Converged Enhanced Ethernet (CEE). CEE was originally developed and thought of by the T11 Working Group to provide lossless connectivity on an Ethernet Layer 2 network. DCB is an IEEE 802.1 standard. DCB is comprised of the following sub-protocols:

* Priority Flow Control (PFC) – A method in which Pause-frames are sent on one of eight lanes. The eight lanes make up the ethernet link which connect from host to FCF or FCoE Transit Switch. In order to prevent dropped FCoE frames, PFC will pause FCoE traffic, and allow others to continue to flow, if congestion is present. A common appoach is to use Priority Group IDs:
  + PGID – Priority Group ID works in conjunction with PFC and ETS to ensure lossless delivery of frames by prioritizing and allocating a bandwidth, which equates to a percentage of the total link speed. PGIDs are commonly used on MXLs, S4810/S4820 switches.
  + iSCSI PGID = 0 0 0 0 1 0 0 0
  + FCoE PGID = 0 0 0 1 0 0 0 0
* Enhanced Transmission Selection (ETS) – Enhanced Transmission Selection provides a mechanism for bandwidth control. It is an effective way to guarantee a minmum amount of bandwidth for
* Quantized Congestion Notification (QCN) - Quantized Congestion Notification is the method by which the switch determines if a link or links are congested. QCN is not commonly used because switchports used for FCoE are usually (at the very least) the speed of 10Gbps.
* DCBX – The Data Center Bridging Exchange Protocol, when enabled, negotiates the DCB parameters of PFC and ETS. Typically the Switch/Fabric dictates a set of possible values for PFC/ETS and passes this down to the host device. The host device, based on its capability, will actively negotiate values for ETS and PFC that match what the switch is capable of.

**Flow Control versus Priority Flow Control** – As previously mentioned, Priority Flow Control will pause FCoE frames from sender to receiver until congestion has been alleviated. It applies to one of the eight lanes, based on the PGID mappings. Flow control is a less granular approach to pause ethernet frames as it applies to the entire link and not one lane of eight. If no other types of traffic flow on the same link from host to switch, regular Flow Control can be utilized. An excellent example of usage would be dedicated switches for an iSCSI SAN, with the certainty of no other traffic traversing the switches. However if granularity is required, such as converging FCoE and LAN traffic, PFC along with DCB must be used.

**NPV and NPIV**

Briefly mentioned earlier, NPV (N\_Port Virtualization), and NPIV (N\_Port ID Virtualization) are two virtualization technologies that are pertinant to Fiber Channel. These two technologies also easily port over to FCoE since the underlying fundamentals of FC are retained.   
  
NPV is more switch focused. Remember that NP\_Port (Node Proxy Port)? A switch in NPV mode, Access-Gateway Mode, or Node Proxy Gateway Mode simply do one thing: Conduct FLOGIs on behalf of other devices. The primary aim for NPV was to reduce the number of Domain IDs in a fabric. In addition to this, a switch in NPV mode does not participate in Fabric Services, which means all Fabric Services would be conducted on a master FC switch.   
  
NPIV is host-focused. A classic example of an implementation of NPIV is on a Dell Storage SC8000 SAN using virtual ports. NPIV virtualizes the N\_Port of a device such that multiple virtual N\_Ports appear on a switch running fabric services. Another example of NPIV is the case of an ESXi host with an NPIV-enabled FC-HBA. The HBA itself has a Node-WWN(nWWN), and a number of Port-WWNs (pWWN). With NPIV enabled, any Virtual Machine has the capability to posses a “virtualized” FC-HBA which provides a virtual pWWN. This pWWN can then be take up to the FC-switch and zoned accordingly to storage device.

**FCoE Port Types**

The more common FC Port types have been translated for use with FCoE. When configuring for FCoE these are the port types that function in an FCoE Network:

* VN\_Port (Virtual Node Port) – Very similar to an N\_Port however, because CNAs are connecting to an FCF, there is no Fiber Channel Fabric Port. All of this becomes “virtualized”. This simply implies that there exisits a mapping of an Ethernet MAC address to a Virtual FC Interface or endpoint in the switch.
* VF\_Port (Virtual Fabric Port) – Very similar to an F\_Port however, because the switchport is Ethernet based, the switchport is emulated to act like an F\_Port.
* VE\_Port (Virtual Expansion Port) – This is similar to the E\_Port however, because an ISL is formed between two FC Switches using the FCP and FC cables, an Ethernet/CAT6A/TwinAX cable will connect two Converged/Ethernet Switches together to extend the Fabric, all while regular Ethernet or LAN traffic can also travel the two swtiches.

**Common FCoE Topologies**

* **Direct Attached VN to VN Port**
* **Switched**
* **Switched with FIP Snooping**
* **FCoE Multi-Hop (VE\_Port to VE\_Port)**

**Storage Protocols Comparison**

As FCoE has already been discussed in detail, some other Storage Networking protocols exist to fulfill the needs of the evolving Data Center. As it has not been clarified earlier, FCoE is a Layer 2 only technology. This means FCoE frames cannot be routed to a remote Data Center using IP connectivity. It can however connect to remote data center by use of some Layer 2 extension technology. Most Internet Service Providers have the ability to extend a VLAN or LAN.

iSCSI, or internet SCSI (SCSI on TCP/IP) runs as a Storage Protocol directly on-top of the Internet Protocol, IP. Because iSCSI utilizes the IP infrastructure, it runs over Ethernet. This means iSCSI can use an exisiting LAN infrastructre. This does not mean that an existing LAN infrastructure is tuned for iSCSI Best Practices, or is tuned for maximum perfomance. iSCSI can make use of either Flow Control or PFC to ensure loss-less delivery of SCSI frames. Without Flow Control or PFC, iSCSI will rely on TCP to retransmit frames. Although TCP guarantees packet delivery (packets contain frames), it’s extremely sub-optimal and detrimental to the performance of a SAN. Because of this sub-optimal nature, this would imply that LUNs would timeout or drop from the end host. This would only app

Fiber Channel has already been discussed in great detail, however it must be pointed out that Fiber Channel is one of the highest performing Storage Network Protocols. As mentioned previously, the Buffer-to-Buffer credit mechanism ensures lossless delivery of Fiber Channel frames. Fiber Channel isn’t limited to just Storage, it can be used for other applications such as Grid-Computing, HPCC, and IBMs FICON.

FCIP or Fiber Channel over IP, uses an existing IP infrastructure to transport FC frames encapsulated in IP over to a remote destination. What’s interesting about FCIP is that it extends the FC Fabric to that remote destination, which simply means two Fabrics are bridged together over IP to form a single fabric. It’s typically used in scenarios where replication of SAN to SAN is ras lequired. FCIP can be additionally used to attached storage to a host. The Cisco MDS 9216i and 9222i Fiber Channel switches support FCIP capabilities.

iFCP or Internet Fiber Channel Protocol is very similar to FCIP in that Fiber Channel is encapsulated in IP. The difference is that iFCP does not bridge SAN Islands, it keeps them separate. iFCP is known to be used as migration strategy to move towards iSCSI and away from Fiber Channel.

**Dell FCoE-Compatible Hardware Platforms**

There are a number of compatible hardware platforms which are enabled to function quite well with FCoE however, each device has limitations based on hardware, software, and firmware. Dell’s Server Portfolio, almost in it’s entirety, can support FCoE. A key piece is what Converged Network Adapter is used due to the additional software and hardware features it offers. Specifically on the networking/switching/fabric side and, at the time of writing with FTOS v9.7, the FCoE-capable switches are:

* S4810 (FCOE Transit/FSB only)
* S5000 (FCOE Transit/FSB, FC Full Fabric, Ethernet)
* MXL (FCOE Transit/FSB, FC Full Fabric, Ethernet)
* S6000 (FCoE Transit/FSB only)
* S4820 (FCoE Transit/FSB only)

**FCoE out-of-the-box and into your Data Center**

Although this technical piece is meant to help understand how FCoE is supposed to work, some guidance on implementing FCoE is important. The three key areas of focus, with detail, are the:

* Fiber Channel Storage Array – A clear example of this would be ensuring an Engineer has racked, cabled, and configured a Dell Storage SC8000 SAN Array, with Fiber Channel. The Fiber Channel Virtual WWNs aren’t available for zoning yet because, the networking needs to be configured. Once the networking has been configured, the Array can turn Virtual Ports on and then Virtual pWWNs appear.
* Hosts – A host, or server, typically would run some sort of operating system (MS Server 2012, or ESXi 5.5), which can recognize and utilize a CNA. Because the CNA has two protocol stacks, Ethernet, and Fiber Channel, built in, the Fiber Channel stack just needs to be enabled through some means of a software or driver installation. A Windows Server 2012, using a Broadcom 57810 Dual-Port 10-Gbps CNA, would require the Broadcom Advance Server Program to be installed. When running the program, the CNA can be recognized and viewed. From within the program, the FC-adapters usually need to be enabled. If a problem exists, chances are a driver update is required or, an appropriate driiver to enable the FC-stack is required. Within Windows, device manager will display, on a dual-port CNA, two Ethernet ports, and two FC ports. At this point FCoE is ready to go. Refer to the manufacturers instructional guide on enabling FCoE for CNAs.
* Networking – For the most part, in an FCoE Deployment, the Network Planning Engineer (NPE) will provide a Field Engineer with configurations for DCB and FCoE. It is always an excellent idea to test out the configurations of the switches in a lab environment. Assuming DCB and FCoE configurations are correct, zoning is the only other piece that a FE should be familiar with. In Appendix [x], a zoning configuration sample is provided with some explanations. On an FCF, prior to Zoning, verify that pWWNs have logged into the fabric. Once the Enodes pWWNs are recognized, zoning can take place and presentation of storage LUNs to hosts should would flawlessly.

**Conclusion (known as the TL ;DR)**

FCoE is great for converging Ethernet for Data services and Fiber-Channel for Storage arrays into a single fabric that is highly redundant.

**S5000 and MXL Zoning**

conf t

\*\*\*\*ENABLE FC SWITCHING\*\*\*\*

feature fc

fc switch-mode fabric-services

\*\*\*\*VERY FLOGIs\*\*\*\*

show fc ns fabric

show fc ns database

\*\*\*\*CREATE ALIASES\*\*\*\*

fc alias [name] \*\*REPEAT FOR MULTIPLE ALIASES\*\*

member [pWWN]

exit

\*\*\*\*CREATE ZONES\*\*\*\*

fc zone [name of zone] \*\*REPEAT FOR MULTIPLE ZONES\*\*

member [alias 1]

member [alias 2]

exit

exit

show fc zone \*\*VERIFY ZONES AND MEMBERS\*\*

\*\*\*\*CREATE ZONESET AND ADD ZONES\*\*\*\*\*

conf t

fc zoneset [name]

member [your zone]

member [your zone 2]

...

member [zone name]

exit

\*\*\*\*ACTIVATE ZONESET\*\*\*\*

fcoe-map default\_full\_fabric

fc-fabric

active-zoneset [name]

exit

exit

exit

\*\*\*\*VERIFY ZONESET is ACTIVE\*\*\*\*

do show fc zoneset active